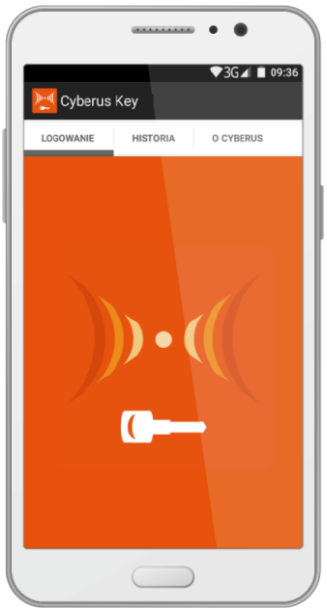
CYBERUSLABS

BEZPIECZNY ŚWIAT




# CYBERUS KEY

## Bezhasłowy system logowania
## Karta Technologii.

**opracowanie:**
**Jack Wolosewicz**
**Dyrektor ds. Technologii Cyberus Labs**

## OPIS TECHNOLOGII

System CYBERUS KEY to pierwszy na świecie, rewolucyjny system bezhasłowego logowania, autoryzacji dostępu oraz identyfikacji stron dokonujących operacji w sieci. System jest wielopoziomową platformą identyfikacji opartą na technologii mobilnej, pozwalającą użytkownikom indywidualnym, komercyjnym oraz instytucjom i agencjom publicznym przeprowadzać w pełni bezpieczne operacje logowania.

Zaletą systemu jest zupełne wyeliminowanie konieczności używania elementów logowania (nazwa użytkownika i hasło), które są przedmiotem ataków cyberprzestępców.

System CYBERUS KEY eliminuje najpoważniejsze zagrożenie dla użytkowników sieci jakim są ataki phishingowe polegające na:

- przejmowaniu dostępu do serwisów internetowych i danych użytkowników,
- poprzez przejęcie dostępu – na wykradanie i przejmowanie tożsamości,
- autoryzację niepożądanych transakcji.

Poprzez swoją konstrukcję system jest odporny na ataki hakerskie.

Jedną z rewolucyjnych zalet systemu jest też to, że pozwala on na identyfikację obu stron przeprowadzanej operacji. Przez to daje użytkownikowi gwarancję, że łączy się z właściwym serwisem.

System pozwala również monitorować i kontrolować logowania się do serwisów, dokonywanie/zatwierdzanie operacji.

Poziom bezpieczeństwa procedury logowania można podnieść, w zależności od wymagań operatora, poprzez zintegrowane z systemem technologie biometryczne (które same z siebie nie stanową gwarancji bezpiecznego dostępu, ale mogą stanowić dodatkowe zabezpieczenia czy metody weryfikacji użytkownika).

## ZALETY I KORZYŚCI Z ZASTOSOWANIA TECHNOLOGII

Przewaga systemu CYBERUS KEY nad obecnymi rozwiązaniami to m.in.:
a) wykorzystanie do procedury logowania jednorazowego kodu dostępu,
b) brak istnienia i konieczności wykorzystania tradycyjnej nazwy użytkownika i hasła oraz dodatkowych zabezpieczeń – kodów TAN i smsów,
c) konstrukcja systemu, technologia wewnętrznej łączności oraz charakterystyka wykorzystywanego sposobu transmisji kodu sprawia, że jest on niemożliwy do przejęcia i późniejszego wykorzystania przez cyberprzestępców,
d) ze względu na szybkość procesu logowania ważność jednorazowego kodu wygasa w czasie poniżej sekundy i nawet w przypadku przejęcia go, po tym czasie staje się on bezużyteczny.

Korzyści:

- identyfikacja obu stron operacji,

- brak wykorzystywania danych identyfikujących użytkownika do procedury logowania,

- wyeliminowanie zagrożenia autoryzowania niepożądanych transakcji czy operacji,

- funkcjonowanie na wszystkich typach urządzeń (telefony komórkowe, tablety, laptopy,

komputery stacjonarne) i systemach operacyjnych iOS, Android,

- możliwość dostosowania funkcjonalności systemu do potrzeb operatora,

- możliwość logowania za pomocą tylko jednego urządzenia,

- logowanie poprzez jedno kliknięcie,

- szybkość całego procesu logowania na poziomie ok. 2 sekund,

- najwyższy poziom zadowolenia użytkownika wraz z najwyższym poziomem bezpieczeństwa oraz pewność dla obu stron operacji,

- możliwość zastosowania systemu do kontroli dostępu do danych i systemów urządzeń,

- funkcjonowanie w różnych warunkach środowiskowych.

## ZASTOSOWANIE RYNKOWE CYBERUS KEY W BRANŻACH

**Energetyka:**
kontrola dostępu do urządzeń, autoryzacja sterowania systemami

**Medycyna, Biotechnologia, Farmacja:**
kontrola dostępu do danych pacjentów, identyfikacja i logowanie pracowników mających dostęp do informacji wrażliwych, autoryzacja operacji prowadzonych przez personel, dostęp pacjentów do swoich kont.

**Wojsko:**
kontrola dostępu do danych wrażliwych, identyfikacja użytkowników, autoryzacja operacji.

**Instytucje finansowe:**
zabezpieczenie dostępu do danych, wyeliminowanie zagrożenia atakami phishingowymi, logowanie użytkowników do kont bankowych, autoryzacja operacji przez pracowników, autoryzacja operacji przez klientów, wykorzystanie kanału do przekazywania treści informacyjnych do właściwych użytkowników.

**E-commerce:**
wyeliminowanie zagrożenia atakami phishingowymi, szybkie tworzenie kont użytkownika, sprzyjające warunki dokonywania transakcji, szybkość dokonywania transakcji wpływająca na ich zwielokrotnienie szybki i bezpieczny dostęp do konta, autoryzacja operacji, wykorzystanie kanału do przekazywania treści informacyjnych do właściwych użytkowników.

**Internet Rzeczy:**
kontrola dostępu do sieci IoT, identyfikacja autoryzowanego użytkownika, zabezpieczenie przed przejęciem kontroli przez urządzenia lub osoby z zewnątrz systemu, autoryzacja pleceń użytkownika.

**Platformy mediowe:**
szybki dostęp do serwisu, wyeliminowanie problemu udostępniania hasła wielu niezarejestrowanym użytkownikom (*„password sharing”*), wykorzystanie kanału do przekazywania treści informacyjnych i reklamowych precyzyjnie dobieranych do właściwych użytkowników.